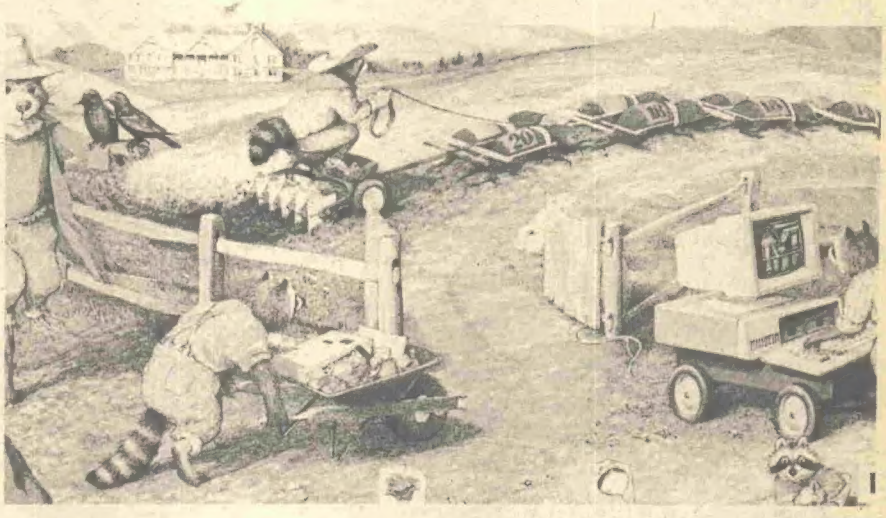
เอนก ศิรจริยาภิวัฒน์

หนทางต่อสู้และป้องกันไวรัส: dBASE และ MIX-I

รู้จักกับพฤติกรรม
และวิธีการแก้ไข
ไวรัส dBASE และ MIX-I



ก่อนเริ่มบทความเรื่องนี้ มีข่าวคราวเกี่ยวกับโปรแกรมที่ใช้ต่อสู้และป้องกันไวรัสออกมาใหม่หนึ่งตัว ท่านผู้อ่านคงจะทราบชื่อเสียงของโปรแกรม Norton Utility นะครับ โปรแกรมที่จะมาช่วยแก้ปัญหาไวรัสได้ดี (ผมหวังไว้เช่นนั้น) ก็คือ Norton anti virus ซึ่งตอนนี้ผมเองยังไม่มีรายละเอียดเกี่ยวกับโปรแกรมตัวนี้ เพียงแต่เห็นในหน้าโฆษณาในวารสารต่างประเทศ ซึ่งเมื่อทางไมโครทราบรายละเอียดแล้วจะไม่พลาดที่จะนำมาเสนอแก่ท่านผู้อ่านแน่นอน สำหรับข่าวคราวฉบับนี้ผมนำมาจากวารสาร VIRUS BULLETIN ซึ่งมีข้อมูลที่ละเอียดพอสมควร สำหรับฉบับหน้าตามกำหนดแล้วต้องเป็นหนทางต่อสู้และป้องกันไวรัสแบบ boot Record และ file ไวรัส แต่ผมขอคั่นด้วยไวรัสชื่อ print screen และไวรัสอีกตัวซึ่งยังไม่ทราบว่าจะตั้งชื่อว่าอะไร เพราะโปรแกรมเช็คไวรัสที่มีเช็คไม่เจอ แต่เท่าที่ดูคร่าว ๆ จะมีโครงสร้างคล้าย sUMsDos พูดถึงไวรัส เรา ๆ ท่าน ๆ คงจะระอาที่จะตามแก้ไขกันจนไม่ไหว ถ้าท่านใดคิดจะลองทำได้โปรดเถอะอย่าปล่อยให้เจ้าไวรัสของท่านหลุดออกมานอกห้องทดลองเลยนะครับ เช่น ไวรัสชื่อลาวดวงเดือนที่กระจายออกมาโดยฝีมือคนไทยเราเอง อีกเรื่องที่อยากจะสะกิดกันไว้ก็คือ อย่าได้เชื่อถือโปรแกรมเช็คไวรัสให้มากเกินควรนะครับ ผมเองเจอกับตัวเองแล้วรู้สึกเศร้าใจ เหตุการณ์ก็คือผมเองได้รับเชิญไปสอน ณ ที่แห่งหนึ่ง ผลของการสอนไม่เป็นไปอย่างคิด เพราะโปรแกรมที่ได้มีขนาดไม่ตรงกับขนาดที่ผมบอก ผมจึงเดินไปดูและพบว่าเป็น sUMsDos รุ่น B-2 แต่ก็โดนต่อว่าไม่มีทางจะเป็นไปได้เพราะผู้อบรมมีโปรแกรมเช็คไวรัส (ซึ่งเช็คได้ประมาณ 5-6 ตัว) ผมเองเลยต้องยอมให้เหตุการณ์เป็นเช่นนั้น เพราะอธิบายซะเหนื่อยพอสมควร (แต่ก็ได้รับการยืนยันว่าไม่มีไวรัส) และด้วยคติอีกอย่างที่ผมชอบมากก็คือ "สู้อะไรก็สู้ได้ แต่อย่าสู้กับความเชื่อของบุคคล" อีกตัวอย่างก็คือโปรแกรมเช็คไวรัสตัวหนึ่งซึ่งผมได้มาไม่นาน (ก่อนหน้าการเขียนบทความคราวก่อนนิดหน่อย) ชื่อว่า VIRUS BLASTER ซึ่งสรรพคุณที่บรรยายไว้หลังหนังสือคู่มือก็คือ เช็คไวรัสได้มากมายรวมถึง 1704 ไวรัสด้วย แต่ผลปรากฏว่าใช้เช็คไวรัส 1704 ที่ผมมีไม่พบ (ถ้าเช็คด้วยโปรแกรม SCAN จะพบ) สะกิดกันนิด ๆ หน่อย ๆ แล้ว เรามาเริ่มบทความกันเลยนะครับ

dBASE Virus

จะพบครั้งแรกราวเดือนมีนาคม 1989 เป็นไวรัสที่ติดกับโปรแกรมนามสกุล .COM และเข้าไปยุ่งกับไฟล์ข้อมูลของ dBASE (.DBF) โดยการทำงานของโปรแกรม dBASE จะเป็นไปอย่างปกติอยู่ระยะหนึ่งประมาณ 3-4 เดือน จะทำให้การทำงานของดีเบสเกิดการผิดพลาดขึ้นเครื่องจะหยุดทำงาน (hang) เมื่อเราใช้งานไฟล์ .DBF ที่ไวรัสเข้าไปยุ่งอยู่แล้ว ไวรัสจะทำงานโดยการเข้าไปดัก INT 21 h ซึ่งเป็นอินเตอร์รัพต์ที่ใช้งานมากที่สุด ส่วนที่ไวรัสต่อนี้เข้าไป

ดักการทำงานของ INT 21 h ก็คือการสร้าง เปิด อ่าน เขียน และปิดไฟล์ รวมทั้งการเรียกโปรแกรมมาปฏิบัติงาน (function 4 Bh)

การแพร่เชื้อ

ไวรัสตัวนี้จะติดกับไฟล์นามสกุล .COM โดยเริ่มแรกไวรัสจะอ่านโปรแกรมที่ไบต์ที่ 2 กับ 3 นำมาคำนวณระยะทางจากต้นไฟล์ (offset) เมื่อได้ระยะจากต้นไฟล์แล้ว จะนำระยะนั้นมาลบออก 2 แล้วอ่านข้อมูล ณ ตำแหน่งถ้าพบว่าข้อมูลที่อ่านได้เป็น E5h, E5h จะถือว่าไฟล์นั้นได้ติดเชื้อไปแล้ว ถ้ายังไม่ติดก็จะทำการต่อโปรแกรมด้วยเชื้อของไวรัสนั้นไว้ท้ายโปรแกรมแล้วแก้จุดเริ่มต้นของโปรแกรมให้ไปทำงานที่ไวรัสก่อน โปรแกรมที่ติดเชื้อจะมีขนาดเพิ่มขึ้น 1864 ไบต์ (จุดสังเกตของ VIRUS ของตัวนี้ก็คือ E5h, E5h จะอยู่ที่ตำแหน่ง 117h จากท้ายโปรแกรม)

การทำงาน

ไวรัสจะดักการทำงานของ INT 21h ดังนี้

1. การสร้างไฟล์ - (ฟังก์ชัน 6Ch, 5Bh, 3Ch)

ไวรัสจะสร้างไฟล์ 1 ตัวคือ BUGS.DAT เพื่อเก็บการสร้างไฟล์ข้อมูลของ dBASE (.DBF) ว่าสร้างเมื่อวันที่เท่าไร โดยเมื่อเราสั่งให้ดีเบสสร้างไฟล์ข้อมูลขึ้นมา ไวรัสก็จะเก็บชื่อนั้นไว้ในไฟล์ BUGS.DAT

2. การเปิดไฟล์ - (ฟังก์ชัน 3Dh)

เมื่อมีการสั่งให้เปิดไฟล์ ไวรัสจะเข้าไปเช็คว่าชื่อไฟล์ที่ทำการเปิดนั้นมีอยู่ใน BUGS.DAT หรือไม่ ถ้ามีก็จะเก็บการเปิดไฟล์ (file handle) ไว้ในหน่วยความจำส่วนของไวรัสเอง

3. การปิดไฟล์ - (ฟังก์ชัน 3Eh)

ไวรัสจะเช็คว่าไฟล์ที่สั่งปิดนั้นมีอยู่บนตารางเก็บการเปิดไฟล์ (file handle) ถ้ามีจะลบการเช็คไฟล์ (file handle) ของไฟล์นั้นทิ้ง

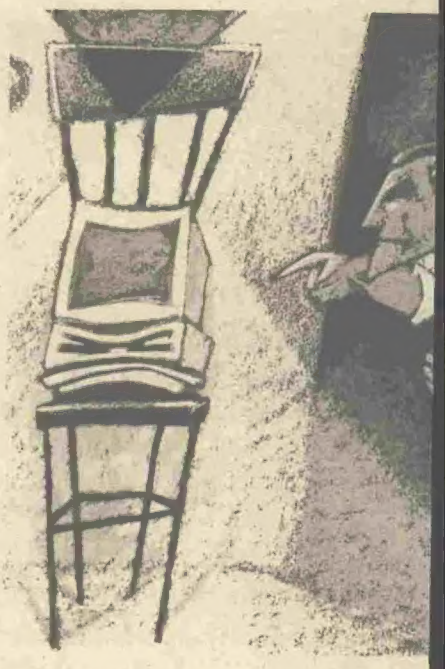
4. การอ่านไฟล์ - (ฟังก์ชัน 3Fh)

เมื่อมีการอ่านไฟล์ ไวรัสจะเช็คว่าไฟล์ที่เช็คนั้นมีอยู่บนตารางเก็บการเปิดไฟล์หรือไม่ ถ้ามีจะทำการสลับข้อมูลระหว่างไบต์คี่กับไบต์คู่ นั้นคือสลับไบต์ที่ 1 กับ 2, ไบต์ที่ 3 กับ 4,...

5. การเขียนไฟล์ - (ฟังก์ชัน 10h)

การเขียนไฟล์ก็เช่นเดียวกันกับการอ่านไฟล์ก็คือ จะมีการสลับไบต์คี่กับไบต์คู่ของไฟล์ข้อมูล จึงทำให้การอ่านและเขียนไฟล์เป็นไปอย่างปกติ แต่กระนั้นก็ยังมีการทำงานผิดพลาดอยู่บ้างในกรณีที่ไฟล์ข้อมูลมีขนาดเป็นเลขคี่เพราะไบต์สุดท้ายจะหายไป ทำให้การทำงานผิดพลาด ซึ่งผลที่ได้มิอาจจะทำนายว่าเป็นอย่างไร ยกเว้นว่าเราจะรู้การทำงานภายในของดีเบสว่ามีวิธีจัดการกับข้อมูลเช่นนี้อย่างไร

เมื่อดูการทำงานแล้ว เราจะรู้ว่างานที่เราทำด้วยดีเบสจะสามารถดำเนินไปเรื่อย ๆ โดยเราไม่มีโอกาสรู้ตัวเลย แต่เมื่อพิจารณาให้ดีจะเห็นว่าไวรัสที่เข้าไปยุ่งกับไฟล์ข้อมูลนี้อันตรายกว่าไวรัสที่ติดกับไฟล์นามสกุล .COM หรือ .EXE เพราะว่าถ้าเรา Backup ข้อมูลแล้วกำจัดไวรัส dBASE ทิ้ง เราจะพบว่าข้อมูลเราไม่สามารถใช้การได้อีกเลย ทั้งนี้เพราะข้อมูลเราถูกสลับตำแหน่งกันอยู่ ซึ่งการสลับตำแหน่งนั้นอาจมิใช่แค่สลับไบต์คู่กับไบต์คี่เท่านั้น ผู้ที่จะตอบคำถามได้ดีที่สุดก็คือผู้ที่รู้การทำงานของไวรัส



dBASE ทั้งหมด ในวารสาร VIRUS BULLETIN เองก็บอกวิธีการแก้ไขเพียงว่าให้พิมพ์ข้อมูลที่มีอยู่ทางเครื่องพิมพ์แล้วค่อยกำจัดไวรัส dBASE ทิ้งเสร็จแล้ว จึงป้อนข้อมูลใหม่ด้วยมือ (keyboard) อีกครั้ง นอกจากผลการสลับข้อมูลของ dBASE ไวรัสแล้ว ไวรัสตัวนี้จะเช็คว่าเดือนที่สร้างไฟล์ BUGS.DAT นั้น ห่างจากวันที่ปัจจุบันมีค่าเป็นลบ (ในกรณีที่ใช้งานข้ามปี เช่น ไฟล์ BUGS.DAT สร้างเดือน 11 ใช้งานจนเดือน 1 ของปีถัดไประยะห่างก็จะเป็น 1-11 =-10) หรือมากกว่าเท่ากับ 3 (เดือนที่สร้างไฟล์ BUGS.DAT กับวันที่ของการใช้คอมพิวเตอร์ห่างกันตั้งแต่ 3 เดือนขึ้นไป) ไวรัสก็จะมีการเรียกใช้ INT 3 และทำงานวนเวียนอยู่ไม่จบ ซึ่งทำให้เครื่องหยุดทำงาน (hang) ไป ซึ่งก่อนจะหยุดทำงานจะมีการรายงานจากโปรแกรม dBASE ปกติว่ามีการผิดพลาดขึ้น ซึ่งเป็นข้อสังเกตว่าดีเบสอาจใช้ INT 3 ทำงานบางอย่างด้วย

การป้องกันและแก้ไข

การแก้ไขนั้นคงมีอยู่วิธีเดียวคือเข้าไปศึกษาว่าไวรัสทำงานอย่างไรบ้าง แล้วเขียนโปรแกรมแก้ขึ้นมา ส่วนวิธีการป้องกันไวรัสตัวนี้ สำหรับการป้องกันนั้นถ้าท่านเป็นโปรแกรมเมอร์ เมื่ออ่านหัวข้อการเข้าสู่หน่วยความจำ คงไม่ใช่เรื่องยากสำหรับเขียนโปรแกรมป้องกันนะครับ ถ้าท่านไม่ใช่โปรแกรมก็ดึงเพื่อน ๆ ที่เป็นโปรแกรมเมอร์มาอ่านบทความนี้ซะหน่อยนะครับ โปรแกรมเมอร์ทั้งหลายคงไม่ใจจืดใจดำกับเพื่อนมนุษย์หรอกครับ

MIX-I

ไวรัสตัวนี้ถูกพบประมาณเดือนกันยายน 1989 โดยไวรัสตัวนี้จะติดเชื้อกับไฟล์นามสกุล .EXE โดยทำให้โปรแกรมต้นฉบับมีขนาดเพิ่มขึ้น 1618 ถึง 1633 ไบต์

การเข้าสู่หน่วยความจำ

ไวรัสจะทำการเช็คหน่วยความจำที่ตำแหน่ง 0:33h ว่าเป็น 77h หรือไม่ ถ้าใช่จะถือว่าหน่วยความจำนั้นมีไวรัส MIX1 อยู่แล้ว ถ้าหน่วยความจำตำแหน่ง 0:33h ไม่ได้มีค่า 77h ไวรัสก็จะแก้ส่วนควบคุมหน่วยความจำของดอส (MCB) เพื่อทำให้ตัวเองเป็นโปรแกรมลักษณะเหมือนกับโปรแกรมประเภทฝังตัวเอง (TSR) และจะทำการดักการทำงานของ Int อยู่ 4 เบอร์คือ Int 8h (system clock), Int 9h (keyboard event interrupt), Int 14h (Asynchronouse communication service), Int 17h (printer service) และ Int 21h (Main Dos service)

การแพร่เชื้อ

ไวรัสจะดักการทำงานของ Int 21h ฟังก์ชัน 4B (การปฏิบัติงานของโปรแกรม /Load and Execute program) โดยถ้าไวรัสพบว่าโปรแกรมที่ถูกเรียกปฏิบัติงานเป็นประเภท EXE และมีขนาดมากกว่าหรือเท่ากับ 8K ก็จะเริ่มทำการแพร่เชื้อโดย

1. ถ้าโปรแกรมเป็นแบบ Read only จะนำค่า attribute Read only ออก โดยไม่มีการเซตกลับให้เป็น Read Only เหมือนเดิม
2. เก็บค่าวันและเวลาของไฟล์นั้นไว้
3. เช็คท้ายไฟล์มีคำว่า MIX1 หรือไม่ ซึ่งเป็นสัญลักษณ์ของไวรัสตัวนี้
4. ทำให้ขนาดของไฟล์หารด้วย 16 ลงตัว (paragraph boundary)
5. เขียนตัวไวรัสต่อท้ายโปรแกรมเดิม
6. แก้ไข EXE file header ให้ตัวไวรัสเริ่มทำงานก่อน
7. นำค่าวันและเวลาของไฟล์เขียนกลับให้เหมือนเดิม

จากการทำงานทั้งหมดนี้จะพบมีลักษณะเหมือนกับ sUMsDos มาก

จึงเป็นที่น่าสังเกตว่า sUMsDos อาจจะเป็นต้นฉบับของไวรัสอีกหลาย ๆ ตัว

การเปลี่ยนแปลงของการสื่อสารแบบอนุกรม (Asynchronous line) และผลของการพิมพ์ (Printer output)

ไวรัสจะทำการเปลี่ยนแปลงข้อมูลที่ส่งออกทางพอร์ตอนุกรม (Asynchronous port) และข้อมูลที่ส่งออกสู่เครื่องพิมพ์ (printer port) โดยใช้ตารางการแปลงข้อมูลดังนี้คือ

ข้อมูลต้นฉบับเป็นดังนี้

LF VT ( )+ – < >
ABEFIOPUY [ ] acefiopsu { }

ผลของข้อมูลที่ออกมาดังนี้

VT LP) (– + > <
BEAPYUFOI] [esapyafco } {

และข้อมูลที่อักษรต่างประเทศหรือตัวอักษรกราฟิกจะถูกแก้ไขด้วย ถ้าไวรัสทำงานจะทำให้คำว่า "Quick Brown Fox" กลายเป็น "Qoysk Eruwn Pux"

การสังเกตอื่น ๆ

หลังจากไวรัสทำงานไป 50 นาที คีย์ Numbers Lock และ Caps lock จะถูกแก้ไข ทุกครั้งที่เรากดคีย์โดยขณะที่ Caps lock ติด, Numbers lock จะดับ และเมื่อป้อนตัวอักษรอีก Caps lock จะดับขณะที่ Numbers lock ติด หลังจากทำงานไป 60 นาที จะมีอักษรหล่นในอัตรา 18 ตำแหน่ง (charactor position) ต่อวินาที ส่วนวิธีการแก้ไขและป้องกันทำเป็นเช่นเดียวกับไวรัส dBASE นะขอรับ